AMENDMENTS TO THE CLAIMS:

This listing of the claims will replace all prior versions, and listings, of the claims in this application.

Listing of Claims:

Claims 1-46, as originally filed, are not amended, and are reproduced below.

1. (Original) A system for monitoring operation of a software program in a network environment, comprising:

an execution component for executing the software program, said execution component being coupled to an isolated network that does not have a direct connection to another network that is not an isolated network;

a monitoring component for obtaining information about actions performed by the software program; and

a network emulation component, coupled to said isolated network, for emulating the behavior of at least a host providing network services; wherein

said execution component and said network emulation component cooperate with said isolated network in order to elicit a behavior of the software program that is detectable by said monitoring component.

2. (Original) A system as in claim 1, where said emulation component further comprises a server programmed so as to return emulated results in response to a request resulting from the software program being executed on said execution component.

3. (Original) A system as in claim 1, where said emulation component is programmed so as to limit access by the software program to only certain resources.

4. (Original) A system as in claim 1, where at least one of said emulation component and monitoring component are programmed so as to provide information about the performance of the software program for the purposes of testing, debugging, performance profiling, or optimization.

5. (Original) A system as in claim 1, where at least one of said emulation component and monitoring component are programmed so as to provide information about actions of the software program for the purposes of reverse engineering or otherwise determining the function and behavior of the software program.

6. (Original) A system as in claim 1, where at least one of said emulation component and monitoring component are programmed so as to provide information about actions of the software program for the purposes of detecting a presence of an undesirable software entity within the software program.

7. (Original) A system as in claim 6, wherein the undesirable software entity comprises at least one of a worm or a virus.

8. (Original) A system as in claim 6, wherein the undesirable software entity comprises a worm that exhibits viral characteristics.

9. (Original) A system as in claim 1, where the elicited behavior of the software program comprises self-replication.

10. (Original) A system as in claim 1, where the elicited behavior of the software program comprises viral or malicious activity.

11. (Original) A system as in claim 2, where said server is programmed to determine what result to return based at least in part on a result of a corresponding real query sent to a corresponding real server on a corresponding real, non-isolated network.

12. (Original) A system as in claim 2, where said server is programmed so as to function as an optimistic host.

13. (Original) A system as in claim 2, where said server comprises at least one of a real or an emulated Web server.

14. (Original) A system as in claim 2, where said server comprises at least one of a real or an emulated http, ftp, imap4, pop3, nntp, news, irc, chat, smtp, mail or mailbox server.

15. (Original) A system as in claim 2, where said server comprises at least one of a real or an emulated router.

16. (Original) A system as in claim 2, where said server comprises at least one of a real or an emulated DNS, WINS, or other Name server.

17. (Original) A system as in claim 2, where said server comprises at least one of a real or an emulated SNMP server.

18. (Original) A system as in claim 2, where said server comprises at least one of a real or an emulated NetBIOS server.

19. (Original) A system as in claim 2, where said server comprises at least one of a real or an emulated server that operates in accordance with SMB, NES or other distributed file system protocols.

20. (Original) A system as in claim 1, where said monitoring component comprises a

monitor programmed to record certain information or types of information that flow across the isolated network as a result of the execution of the software program.

21. (Original) A system as in claim 1, where said monitoring component comprises a monitor programmed to record at least one of certain operating system level or application level activities or types of activities that occur in real or emulated host computers as a result of the execution of the software program.

22. (Original) A system as in claim 2, where said monitoring component comprises a monitor programmed to record at least certain activities or types of activities that occur in said server as a result of the execution of the software program.

A1

23. (Original) A system as in claim 1, where said monitoring component comprises at least one event handler programmed so as to obtain control when certain events or types of events occur.

24. (Original) A system as in claim 23, where the certain events or types of events comprise at least one of creation of a new file in a filesystem, a receipt of mail, an opening of mail, a posting of news, an opening of a new socket connection, an execution of a particular application, and an alteration of a system registry.

25. (Original) A system as in claim 1, where said emulation component further comprises a system activity emulation component for emulating typical or specific activity on at least one of said isolated network and a real or emulated host computer.

26. (Original) A system as in claim 25, where the typical or specific activity comprises at least one of sending mail, opening mail, opening or execution of a mail attachment, entry of keystrokes, issuing of user commands, execution of a particular application, rebooting a real or emulated host computer, restarting a real or emulated host computer, reinitialization of a real or emulated host computer, posting of news, participation in real-time messaging, and a transfer of

files.

27. (Original) A system for eliciting a desired behavior from a software program, comprising:

an emulated data communications network having at least one emulated network server coupled thereto, said at least one emulated network server responding to requests received from said emulated data communications network;

an emulated host computer coupled to said emulated data communications network, said emulated host computer for executing the software program, the software program operating to originate requests to said emulated data communications network;

at least one emulated goat computer coupled to said emulated data communications network; and

at least one monitor for detecting an occurrence of the desired behavior in at least one of said emulated network server, said emulated host computer, and said at least one emulated goat computer.

28. (Original) A system as in claim 27, wherein said at least one emulated network server operates as an optimistic server when responding to requests received from said emulated data communications network.

29. (Original) A system as in claim 27, wherein the desired behavior is indicative of a presence of an undesirable software entity within the software program.

30. (Original) A system as in claim 29, wherein the undesirable software entity comprises at least one of a worm or a virus.

31. (Original) A system as in claim 29, wherein the undesirable software entity comprises a worm that exhibits viral characteristics.

32. (Original) A system as in claim 27, where the desired behavior comprises self-replication.

33. (Original) A system as in claim 27, where the desired behavior comprises viral activity or malicious activity.

34. (Original) A system as in claim 27, wherein said monitor operates to detect at least one of a creation of a new file, a receipt of mail, an opening of mail, a posting of news, an opening of a new socket connection, an execution of a particular application, and an alteration of a system registry.

35. (Original) A system as in claim 27, where at least one of said emulated host computer and said monitor are programmed so as to provide information about the performance of the software program for the purposes of testing, debugging, performance profiling, or optimization.

36. (Original) A system as in claim 27, where at least one of said emulated host computer and said monitor are programmed so as to provide information about the performance of the software program for the purposes of reverse engineering or otherwise determining the function and behavior of the software program.

37. (Original) A computer program embodied on at least one computer-readable medium for executing a method for eliciting a behavior from a software program, the method comprising steps of:

emulating a data communications network having at least one emulated network server coupled thereto, said at least one emulated network server operating to respond to requests received from said emulated data communications network;

emulating a host computer coupled to said emulated data communications network, said emulated host computer executing the software program, the software program operating to originate requests to said emulated data communications network; and

detecting an occurrence of the behavior in at least one of said emulated network server and said emulated host computer.

38. (Original) A computer program as in claim 37, and further comprising a step of emulating at least one goat computer coupled to said emulated data communications network, and wherein the step of detecting an occurrence of the behavior detects the occurrence of the behavior in said at least one goat computer.

A1

39. (Original) A computer program as in claim 37, wherein the elicited behavior is indicative of a presence of an undesirable software entity within the software program.

40. (Original) A computer program as in claim 38, wherein the elicited behavior is indicative of a presence of an undesirable software entity within the software program, and wherein the undesirable software entity comprises at least one of a worm, a virus, or a worm that exhibits viral characteristics.

41. (Original) A computer program as in claim 37, wherein the elicited behavior comprises self-replication.

42. (Original) A computer program as in claim 37, wherein the elicited behavior comprises worm-like or virus-like behavior.

43. (Original) A computer program as in claim 37, wherein said step of detecting operates to detect at least one of a creation of a new file, a receipt of mail, an opening of mail, a posting of news, an opening of a new socket connection, an execution of a particular application, and an alteration of a system registry.

44. (Original) A computer program as in claim 37, wherein said at least one emulated network server operates as an optimistic server.

45. (Original) A computer program as in claim 37, wherein said method provides information about the performance of the software program for the purposes of testing, debugging, performance profiling, or optimization.

46. (Original) A computer program as in claim 37, wherein said method provides information about the performance of the software program for the purposes of reverse engineering or otherwise determining the function and behavior of the software program.